CLAIMS

What is claimed is:

1. A method comprising:

loading port authentication firmware instructions in a supplicant system; and

authenticating a network port hosted by an authenticator system to which the supplicant system is linked via execution of the port authentication firmware instructions on the supplicant system.

2. The method of claim 1, wherein the network port is authenticated during a pre-boot phase.

3. The method of claim 2, further comprising loading an operating system image into the supplicant system over a network that is accessed via the network port that is authenticated.

4. The method of claim 1, wherein the network port is authenticated during an operating system (OS)-runtime phase.

5. The method of claim 4, wherein network port authentication is performed by executing the port authentication firmware using a hidden execution mode that is transparent to an operating system running on the supplicant system during the OS-runtime phase

6. The method of claim 5, wherein the hidden execution mode is a system management mode (SMM).

7. The method of claim 6, wherein the firmware instructions are embodied as one or more SMM handlers.

8. The method of claim 7, further comprising:

asserting one of an SMI (system management interrupt) or PMI (Processor Management Interrupt) on a processor of the supplicant on a periodic basis;

dispatching said one or more SMM handlers to handle the SMI or PMI event via operations including,

determining if a network port needs to be authenticated; and, in response thereto,

authenticating the network port.

9. The method of claim 1, wherein port authentication is performed using the EAPOL (extensible authentication protocol over local area network) protocol.

10. The method of claim 1, wherein the port is authenticated using an access/challenge scheme.

11. The method of claim 10, wherein the access/challenge scheme employs a Transport Layer Security (TLS) challenge response in which authentication is determined based on credentials provided by the supplicant system.

12. The method of claim 11, wherein the TLS challenge response employs credentials stored in a Trusted Platform Module (TPM), and wherein the method further comprises retrieving the credentials from the TPM.

13. The method of claim 1, wherein a determination of whether a port is authenticated is made by an authentication server that is linked in communication with the authenticator system.

14. The method of claim 1, further comprising providing an callable interface via which a port authentication process can be invoked.

15. A method comprising:

executing instructions comprising port authentication code via a baseboard management controller (BMC) in a supplicant system to perform port authentication of a authenticator system port to which the supplicant system is linked in communication.

16. The method of claim 15, wherein the port authentication code is stored in a non-volatile storage device coupled to the BMC, the method further comprising loading the port authentication code into the BMC for execution.

17. The method of claim 15, wherein the port authentication is performed during an operating system runtime phase.

18. A method comprising:

retrieving authentication credentials pertaining to a supplicant system during a pre-boot phase of the supplicant system;

passing the authentication credentials to an operating system running on the supplicant system during an operating system runtime phase; and

authenticating a network port to which the supplicant system is connected via use of the authentication credentials.

19. The method of claim 18, wherein the operating system is compliant with the IEEE 802.1x port-based network access control standard and authenticates the network port via an 802.1x authentication protocol.

20. The method of claim 19, wherein the network port is authenticated using a Transport Layer Security (TLS) challenge response in which authentication is determined based on the authentication credentials.

21. A machine-readable media on which firmware instructions are stored, which when executed by a supplicant system perform operations including:

authenticating a network port hosted by an authenticator system to which the supplicant system is linked.

22. The machine-readable media of claim 21, wherein the media comprises a firmware storage device.

23. The machine-readable media of claim 21, wherein the firmware instructions comprise at least one system management mode (SMM) handler that is executed by a processor of the supplicant system while operating in SMM.

24. The machine-readable media of claim 21, wherein the network port is authenticated during a pre-boot phase of the supplicant system.

25. A supplicant system comprising:

a processor;

a network interface, coupled to the processor; and

a flash device coupled to the processor, having firmware instructions stored therein that when executed on the processor perform operations including:

authenticating a network port hosted by an authenticator system to which the supplicant system is linked in communication via the network interface.

26. The supplicant system of claim 25, further comprising a trusted platform module coupled to the processor, to store authentication credentials employed for authenticating the network port.

27. The supplicant system of claim 25, wherein the processor includes a hidden execution mode and the network port is authenticated during an operating system runtime phase via execution of firmware instructions under the hidden execution mode.

28. A supplicant system comprising:

a baseboard management controller (BMC);

a network interface, coupled to the baseboard management controller; and

machine-executable instructions stored on the supplicant system, which when executed on the BMC perform operations including:

authenticating a network port hosted by an authenticator system to which the supplicant system is linked in communication via the network interface.

29. The supplicant system of claim 28, further comprising a trusted platform module coupled to the BMC, to store authentication credentials employed for authenticating the network port.

30. The supplicant system of claim 28, wherein the machine-executable instructions are stored in one of the BMC or a non-volatile storage device coupled to that BMC.